Amendments To the Claims:

Please amend the claims as shown. Applicants reserve the right to pursue any cancelled claims at a later date.

1.-23. (cancelled)

24. (new) A method for transmitting data, comprising:

inputting first data originating from a stochastic process into at least first and second users of a communication network;

generating in each of the at least first and second users first and second symmetrical encryption keys based on the first data;

storing the first and second symmetrical encryption keys in each of the at least first and second users for transmitting encrypted data between the at least first and second users; and

transmitting the encrypted data between the at least first and second users, wherein the encrypted data are generated by changing between the first and second symmetrical encryption keys in a chronological sequence and applying the first respectively second symmetrical encryption key to data to be transmitted.

25. (new) The method as claimed in claim 24, wherein generating the first and second symmetrical encryption keys includes generating a plurality of first data by applying a plurality of combinatorial operations to data originating from the stochastic process.

26. (new) The method as claimed in claim 24, wherein the first data are transmitted over the communication network.

27. (new) The method as claimed in claim 24, wherein the first data are obtained by acquiring at least one measured value from the stochastic process.

28. (new) The method as claimed in claim 24, wherein the stochastic process includes a time-variable parameter of an automation system.

29. (new) The method as claimed in claim 24, wherein the first data are obtained from a Least Significant Bit position related to at least one measured value.

30. (new) The method as claimed in claim 24, wherein each of the at least first and second users acquires data originating from the stochastic process for generating the first data.

31. (new) The method as claimed in claim 30, wherein the first data are generated by applying predefined combinatorial operations to the data originating from the stochastic process.

32. (new) The method as claimed in claim 30, wherein the acquired data originating from the stochastic process are transmitted over the communication network.

33. (new) The method as claimed in claim 24, wherein the first and second symmetrical encryption keys are generated upon a request by a master user of the communication network.

34. (new) The method as claimed in claim 24, wherein the first and second symmetrical encryption keys are generated at predetermined times or after a lapse of a predetermined time interval.

35. (new) The method as claimed in claim 26, wherein the first data are transmitted over the communication network at a time of low utilization of the communication network.

36. (new) The method as claimed in claim 30, wherein the acquired data originating from the stochastic process are transmitted over the communication network at a time of low utilization of the communication network.

37. (new) The method as claimed in claim 26, wherein the first data are transmitted using an asymmetrical encryption method.

38. (new) The method as claimed in claim 30, wherein the acquired data originating from the stochastic process are transmitted using an asymmetrical encryption method.

39. (new) A computer program, comprising software modules configured to execute the following steps:

inputting first data originating from a stochastic process into at least first and second users of a communication network;

generating in each of the at least first and second users first and second symmetrical encryption keys based on the first data;

storing the first and second symmetrical encryption keys in each of the at least first and second users for transmitting encrypted data between the at least first and second users; and

transmitting the encrypted data between the at least first and second users, wherein the encrypted data are generated by changing between the first and second symmetrical encryption keys in a chronological sequence and applying the first respectively second symmetrical encryption key to data to be transmitted.

40. A communication system, comprising:

at least first and second users;

a communication network for transmitting data between the at least first and second users;

an input mechanism for inputting first data originating from a stochastic process into the at least first and second users of a communication network;

an encryption key generator for generating in each of the at least first and second users first and second symmetrical encryption keys based on the first data; and

a storage unit for storing the first and second symmetrical encryption keys in each of the at least first and second users for enabling transmission of encrypted data between the at least first and second users, wherein the encrypted data are transmitted between the at least first and second users, and the encrypted data are generated by changing between the first and second symmetrical encryption keys in a chronological sequence and applying the first respectively second symmetrical encryption key to data to be transmitted.

41. (new) The communication system as claimed in claim 40, wherein the communication network is a public network.

42. (new) The communication system as claimed in claim 40, wherein the communication network is the internet, and the first or second user is a master user for triggering the generating of the first and second symmetrical encryption keys by issuing a request via the internet.

43. (new) The communication system as claimed in claim 40, wherein the communication network is an Ethernet.

44. (new) The communication system as claimed in claim 43, wherein the first or second user is a master user configured to output a command onto the Ethernet for triggering the generation of the first and second symmetrical encryption keys.